

REMARKS

This Response is submitted in reply to the Final Office Action dated June 16, 2009 in conjunction with the enclosed Request for Continued Examination. Claims 1 and 3 to 5 are pending in this application. Claim 2 stands canceled. Claims 1 and 3 to 5 are hereby amended. Claims 1 and 3 to 5 are in independent form. Please charge Deposit Account No. 02-1818 for all payments due in connection with this Response.

As noted above, Applicant has filed a Request for Continued Examination with this Response. Accordingly, Applicant requests that the Examiner provide an upcoming Office Action which will "... identify any claims which he or she judges, as presently recited, to be allowable and/or ... suggest any way in which he or she considers that rejected claims may be amended to make them allowable" in accordance with §707.07(d) of the MPEP.

The Office Action rejected Claims 1 and 3 to 5 under 35 U.S.C. 103(a) as being obvious over WO 2003/038571 to Ochi et al. in view of U.S. Patent No. 5,345,508 to Lynn et al. ("Lynn"). In view of the amendments made herein, Applicant respectfully disagrees with these rejections.

Please note that for purposes of this Response, U.S. Patent No. 7,275,161 to Ochi et al. ("Ochi") is taken to be the English language equivalent to WO 2003/03857 and will be referred to herein, as done by the Patent Office.

Ochi discloses a device for mutual authentication and content protection. The Abstract of Ochi discloses:

A data processing device 10 is composed of a data storage unit 11 that stores first authentication data, second medium authentication data generated by applying a predetermined encryption to the first medium authentication data, and second device authentication data generated by applying the predetermined encryption to first device authentication data; a medium authentication data transmission unit 12 transmits the first medium authentication data; an encrypted data reception unit 13 receives first encrypted data; an authentication unit 14 authenticates an information recording medium 30 when the first encrypted data and the second medium authentication data are identical; a device authentication data reception unit 15 receives the first device authentication data; and a device authentication data transmission unit 16 transmits the second device authentication data. Mutual authentication processing can be performed without the data processing device having a unit for encrypting, and by using data each time. Developers of various types of software can perform data transfer operation checking, debugging and the like without the risk of secret information being leaked.

Lynn discloses an apparatus for variable-overhead cached encryption. The Abstract of Lynn discloses:

A digital encryption structure allows the varying of the computational overhead by selectively reusing, according to the desired level of security, a pseudorandom encoding sequence at the transmitter end and by storing and reusing pseudorandom decoding sequences, associated with one or more transmitters at the receiver end. A public initialization vector is combined with a secret key to produce a deterministic sequence from a pseudorandom number generator. This pseudorandom sequence in turn, is used to convert plaintext to ciphertext. The sequence may be selectively reused by storing the sequence to a transmitter memory cache and iteratively reading the sequence from memory according to a counter which controls the level of security of the encryption system. The ciphertext is decrypted on the receiver end by invertibly combining the ciphertext with the same pseudorandom sequence used by the transmitter to originally encode the plaintext. The pseudorandom sequence is independently generated by the receiver end using the original key and initialization vector used in the transmitter end. Once generated in the receiver, the pseudorandom sequence is stored in a receiver cache for reuse with each iterative use of the stored transmitter pseudorandom sequence.

Page 4 of the Office Action stated:

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the data processing system disclosed by Ochi to use variable overhead cached encryption for encrypting the authentication data transmitted between the data processing device and the information recording medium such as that taught by Lynn in order to perform high speed encryption of the transmitted data (See Lynn col. 2 lines 47-51).

Applicant respectfully submits that even if properly combined, neither Ochi or Lynn individually, nor the information processing apparatus resulting from a combination of Ochi and Lynn disclose "at least one memory device storing instructions, which when executed by the at least one processor, cause the at least one processor to . . . (f) determine whether an instruction to have said initializing vector supplied is given by an external apparatus; (g) if the instruction to have said initializing vector supplied is given by said external apparatus: (i) generate said initializing vector; (ii) reset the number of times having been counted; and (iii) transfer said initializing vector to said external apparatus; (h) if the instruction to stop the transfer of said data is given, output to said external apparatus a message indicating that the transfer of said data is stopped; (i) after said instruction to generate the initializing vector is given, determine whether said external apparatus requests a reissue of said initializing vector; and (j) if the external

apparatus requests the reissue of said initializing vector: (i) generate a reissue initializing vector; (ii) reset the number of times having been counted; and (ii) transfer said reissue initialing vector to said external apparatus.” Additionally, it would not have been obvious to one of ordinary skill in the art to modify Ochi and Lynn to result in such an information processing apparatus without reasonably being construed as improper hindsight reconstruction. On the other hand, the information processing apparatus of amended independent Claim 1 includes, among other elements, “at least one memory device storing instructions, which when executed by the at least one processor, cause the at least one processor to . . . (f) determine whether an instruction to have said initializing vector supplied is given by an external apparatus; (g) if the instruction to have said initializing vector supplied is given by said external apparatus: (i) generate said initializing vector; (ii) reset the number of times having been counted; and (iii) transfer said initializing vector to said external apparatus; (h) if the instruction to stop the transfer of said data is given, output to said external apparatus a message indicating that the transfer of said data is stopped; (i) after said instruction to generate the initializing vector is given, determine whether said external apparatus requests a reissue of said initializing vector; and (j) if the external apparatus requests the reissue of said initializing vector: (i) generate a reissue initializing vector; (ii) reset the number of times having been counted; and (ii) transfer said reissue initialing vector to said external apparatus.”

No new matter has been added by the amendments. Support for the amendments can be found in the Specification, for example, in at least paragraphs [0174] to [0176] and Figs. 12 and 13 of the present application.

For at least these reasons, it is respectfully submitted that independent Claim 1 is patentably distinguished over Ochi and Lynn and in condition for allowance. Independent Claims 3 to 5 each include certain similar elements to independent Claim 1. For reasons similar to those discussed above with respect to independent Claim 1, independent Claims 3 to 5 are each patentably distinguished over Ochi and Lynn and in condition for allowance.

An earnest endeavor has been made to place this application in condition for formal allowance, and allowance is courteously solicited. If the Examiner has any questions regarding this Response, Applicant respectfully requests that the Examiner contact the undersigned.

Respectfully submitted,

K&L GATES LLP

BY



Thomas C. Basso

Reg. No. 46,541

Customer No. 29175

Phone: (312) 807-4310

Dated: August 11, 2009